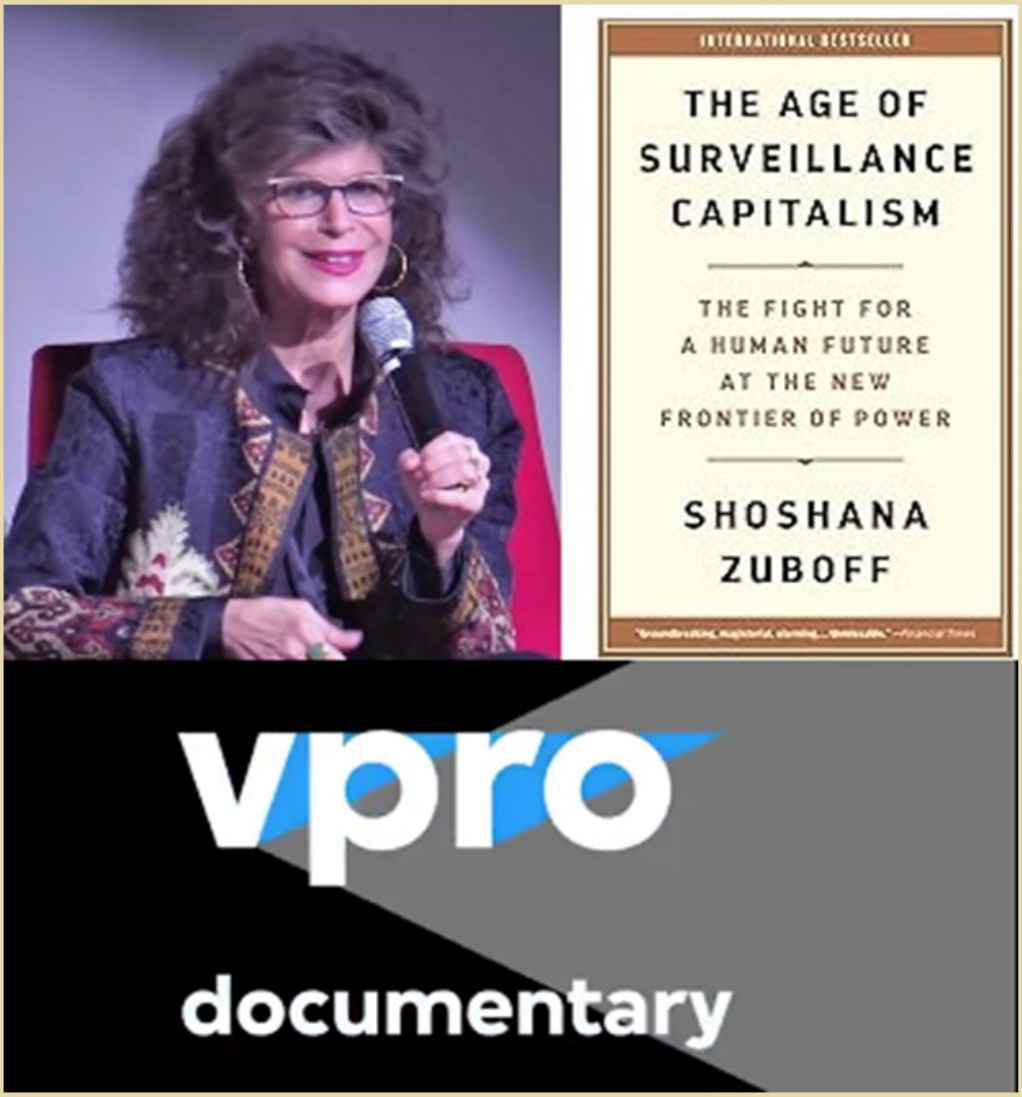
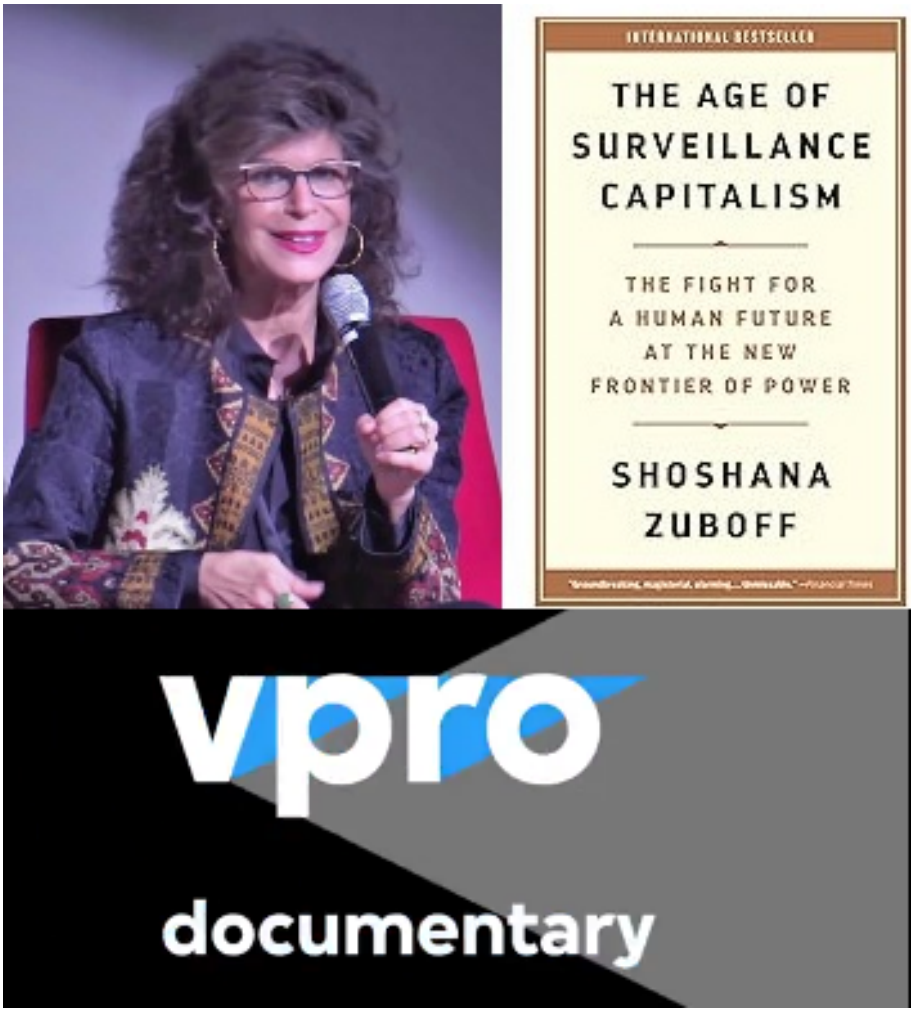
Shoshana Zuboff on surveillance capitalism VPRO Documentary



Shoshana Zuboff on Surveillance Capitalism VPRO Documentary

https://www.bitchute.com/video/HVsHT0FYsfEj/ 50 minutes

https://www.youtube.com/watch?v=hIXhnWUmMvw



Harvard professor Shoshana Zuboff wrote a monumental book about the new economic order that is alarming. "The Age of Surveillance Capitalism," reveals how the biggest tech companies deal with our data. How do we regain control of our data? What is surveillance capitalism? In this documentary, Zuboff takes the lid off Google and Facebook and reveals a merciless form of capitalism in which no natural resources, but the citizen itself, serves as a raw material. How

can citizens regain control of their data? It is 2000, and the dot.com crisis has caused deep wounds. How will startup Google survive the bursting of the internet bubble? Founders Larry Page and Sergey Brin don't know anymore how to turn the tide. By chance, Google discovers that the "residual data" that people leave behind in their searches on the internet is very precious and tradable. This residual data can be used to predict the behavior of the internet user. Internet advertisements can, therefore, be used in a very targeted and effective way. A completely new business model is born: "surveillance capitalism."

While industrial capitalism exploited and controlled nature with devastating consequences, surveillance capitalism exploits and controls human nature with a totalitarian order as the endpoint of the development.

Premise

Zuboff states that surveillance capitalism "unilaterally claims human experience as free raw material for translation into behavioural data [which] are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into *prediction products* that anticipate what you will do now, soon, and later." She states that these new capitalist products "are traded in a new kind of marketplace that I call *behavioural futures markets*."

In a capitalist society, information, such as a user's likes and dislikes gathered when accessing a platform like Facebook, or from any other kind of sensor that serves as an internet touch point to data-stream, is information that can be used by that company to better the experience of a user by feeding them information that data obtained from their previous activity would have shown them to be interested in. It can also infer many things about the individual that extend far beyond the terms and conditions of use.

This in many ways can be done through the use of an algorithm that analyses information. The danger of surveillance capitalism is that

platforms and tech companies claim ownership of private information because it is free for them to access, claiming private experience as 'raw material' for data factories. There is very little supervision or actual laws by governments and users themselves. Because of this, there has been backlash on how these companies have used the information gathered. For example, Google, which is said to be "the pioneer of surveillance capitalism"[] introduced a feature that used "commercial models … discovered by people in a time and place" This means that not only are commercials being specifically targeted to you through your phone, but now work hand in hand with your environment and habits such as being shown an advertisement of a local bar when walking around downtown in the evening. Advertising attempts this technical and specific can easily have an impact on the one's decision-making process in the activities they choose and in political decisions. Thus the idea that these companies seemingly go unchecked whilst having the power to observe and control thinking is one of the many reasons tech companies such as Google themselves are under so much scrutiny and criticism.

Furthermore, Zuboff writes, the freedom allotted to tech companies comes from the idea that "surveillance capitalism does not abandon established capitalist 'laws' such as competitive production, profit maximization, productivity and growth", as they are principles any business in a capitalistic society should aim to excel in, in order to be competitive. Zuboff claims in an article that "new logic accumulation … introduces its own laws of motion". In other words, this is a new phenomenon in capitalistic operations that should be treated as such and be instilled with its own specific restrictions and limitations. Lastly, as invasive as platforms have been in terms of accumulating information, they have also led to what is now called a "sharing economy", Van Dijck (2018) in which digital information can be obtained by individuals carrying out their own surveillance capitalism through the aid of platforms themselves. Thus "individuals can greatly benefit from this transformation because it empowers them to set up business", Van Dijck (2018). Small businesses will also benefit in potentially growing faster than they would have without knowing consumer demands and wants but would need to pay corporations for access to knowledge. This leaves surveillance capitalism as an exceptionally useful tool for businesses, but also an invasion of privacy to users who do not want their private experience to be owned by a company.

Our ignorance is their bliss.

What is not discussed are the political consequences, how technocrat billionaires band together to create narratives and public expectations in advance regarding technologies they would like to be embraced but unregulated, like AI, quantum computing, cool fusion clean nuclear power, antigravity technology, cryptocurrencies, etc. They have lots of money to spend, back room corporate goals and clearly documented service-to-self motives to get things in their pocket before a legal framework is established protecting the public good. The out of sight, out of mind, profits first regardless of legal consequences outlook efforts to control the planet are discussed here, politely called by names like obfuscation and denial. Morality is at a minimum, reassurances are tokenisms, but where is life, liberty and the pursuit of happiness with a loving and open heart? How do you implement trust, beauty, and fair play for all in a world dominated by price tags?

VPRO Video Transcript:

HOST: Harvard professor Shoshana Zuboff is sometimes called the Karl Marx of our time. Her monumental book *The Age of Surveillance Capitalism* exposed the dubious mechanisms of our digital economy. According to Zuboff, our personal and private experiences have been hijacked by Silicon Valley and used as the raw material for extremely profitable digital products.
SHOSHANA: The term surveillance capitalism is not an arbitrary term. Why surveillance? Because it must be operations that are engineered as undetectable, indecipherable, cloaked in rhetoric that aims to misdirect, obfuscate and just downright bamboozle all of us all the time.
Tract Voice: Connecting them.
Tract Voice 2: Don't be evil.
Tract Voice: Connecting them is humanity. Don't be evil. Humanity, humanity.
Tract Voice 3: It's about empowerment of the individual.
ZUCKERBERG: The future is private.
HOST: What really happens with your Facebook photos? Why are there hidden microphones in Google Nest? And Pokemon Go

exposed as child molesters? In this episode of Backlight, Shoshana Zuboff reveals how Silicon Valley deceives us so well.

QUESTIONER: How all this comes into play when I buy a pair of shoes on the internet?

SHOSHANA: Well, you know, some people will say to me, but Professor Zuboff, I like those targeted ads. They're so useful. Or I enjoy personalized services. Sometimes people will say, you know, I have nothing to hide. So I don't care what they take. Each one of these statements is a profound misconception of what's really going on. We think that the only personal information they have about us is what we've given them. And we think we can exert some control over what we give them. And therefore, we think that our calculation, our trade-off here, is something that is somehow under our control that we understand it. What's really happening is that we provide personal information, but the information that we provide is the least important part of the information that they collect about us.

HOST: Thanks to their navigation and search engine, Google knows where we are all the time and what we think. Facebook knows our hobbies, preferences and friends because they retrieve a lot of information from the digital traces we leave behind unwittingly. Spelling errors in your search terms, which colour buttons you prefer, how fast you type, how fast you drive, residual data.

SHOSHANA: Way back at the beginning, back in the year 2000, 2001, 2002, back in those days, these data were considered just extra data. They were considered waste material. And people called them things like digital exhaust or data exhaust. Eventually, it was understood that these so-called waste materials harbored these rich predictive data.

GOOGLE EMPLOYEE: The search generation we retain, we do for quality purposes. So, for example, the Google Spell Checker, our did you mean feature that appears on Google, has been built using long periods of data around someone issuing a query and then issuing another corrected query right after that and us learning those corrections. And it actually takes more than 30 days worth of data to build the world class spell corrector that we have.

SHOSHANA: The companies like to say, we collect data so that we can improve our service. And that's true. They collect data and some of it is used to improve the service to you. But even more of it is analyzed to train what they call models, patterns of human behaviour. So once I have big training models, I can see how people with these characteristics typically behave over time. And that allows me to fit your data right into that arc and to predict what you're likely to do not only now, but soon and later. This is what I call *behavioral surplus*. These data streams filled with these rich predictive data. Why surplus? Because right from the start, these were more data than was required to improve products and services.
HOST: Once you have the behavioral surplus, the comprehensive behavioral data of hundreds of millions of people, you can start predicting the preferences of specific groups. Think popular shoes for mail managers or the preferred restaurant of a group of people sharing the same zip code.
QUESTIONER: Maybe they do a prediction where I have dinner tonight. Or how can I imagine what they will predict about me?
SHOSHANA: Well, you know, at the simplest level, they may predict the kind of food you're in the mood for right now and then sell that prediction, auction that prediction to their business customers in the restaurant business who will then send you a very quick ad. We know you're in the mood for a delicious pasta dish tonight. We can invite you to a restaurant and here's a discount coupon.
QUESTIONER: There are some people who are saying, well, it's very improbable that those targeted ads really can achieve something because people have their own will and they will not buy some shoes just because there is an ad in front of them. **SHOSHANA:** You know, I think one of the misconceptions that it's really important for us to move away from is that surveillance capitalism is something that is only manifest in our lives when we're online or somehow it's only restricted to online targeted advertising. It's easy for us to say, oh, these things don't affect me. The fact is, this is being conducted at a layer that is not accessible to us.
HOST: We have no idea what today's algorithms can predict about us or what behavioral data they used to do it. A simple thing like

buying a certain kind of shampoo can divulge essential information about us. For example, the New York Times reported a case of a supermarket chain that a new a girl was pregnant even before she did or was prepared to share the news. The market's algorithms discovered that the girl switched from fragrant shampoos to more neutral smelling products.

Since the olfactory sensors of pregnant women become stronger, the market algorithm assumed this girl must be pregnant. Her father didn't know until he was repeatedly sent special offers for baby products. Thanks to the analysis of trillions of terabytes of behavioral data that we unwittingly leave around the digital domain, Big Tech sometimes knows us better than we know ourselves.

SHOSHANA: They can predict things like our personality, our emotions, our sexual orientation, our political orientation, a whole range of things that we never ever intended to disclose.

HOST: The predictive value that Big Tech can glean from residual data is huge. The family photos we post on our Facebook pages contain residual data from which vast amounts of valuable knowledge can be distilled.

SHOSHANA: Let's say I put my children's birthday party photo album on the web on the Facebook pages. What we don't understand is that the most important thing there are not the photos per se. It's the predictive signals that these companies can lift from the photos. It's not just my face, but it's allowing them to have the face so that they can analyze the hundreds of muscles in my face.

HOST: Uploading innocent snapshots on your Facebook page can have unforeseen consequences. Our faces, for example, are used to train algorithms to recognize facial features. And we have absolutely no idea what that facial recognition software is used for.

SHOSHANA: These data streams with these rich predictive signals are fed into the new factories, the computational factories, analyzed for predictions of human behavior. And these predictions are then sold. Who are they sold to? They're not sold to us. We are not the customers. They're sold to businesses, to business customers who want to maximize our value to their business, whatever it may be.

They use information from our faces, which we've given billions and billions of photos to Facebook to train models for facial recognition. Those models are then sold to military operations, some of them in China. And those Chinese operations do many things, including imprisoning the Uighar, a subset of the Uighar Muslim population in China in what is rightly regarded as an open-air prison, where they actually don't have to have people behind bars because they track and follow them constantly through facial recognition.

HOST: The knowledge obtained from our residual data can be sold to anyone. Facial recognition software, for instance, might be sold to a Chinese company that supports the oppression of the Uighars in China, all that helps track down advocates of democracy in Hong Kong. That way, our precious family photos might be used by Facebook to facilitate authoritarian regimes. And our privacy is guaranteed, because it's not our faces that are sold. It's the residual data scraped off them.

SHOSHANA: It's very difficult to have a concept of this for a very good reason. It's not because we're stupid. It's because these processes have been disguised. They operate in stealth. They have been engineered to be indecipherable, to be undetectable, to create ignorance in a vast group of all of us that they call users.

Our ignorance is their bliss. There are some things that have broken through into the public view that we do know about. So let's talk about Facebook's massive scale contagion experiments. And this is where Facebook experimented with subliminal cues planted in its Facebook pages that would actually influence offline real world behavior and emotions to see if they could make people feel happier or sadder using subliminal cues with language manipulation and word manipulation and so on.

Well, when the experimenters wrote up this work in the very prestigious scholarly journals that published the results of these experiments, they emphasized two key findings.

Number one, we now know that we can manipulate subliminal cues in the online context to change real world behavior or real world emotion. We know that we can be successful at doing this.

Number two, we can exercise this power, these methods, while bypassing user awareness.
Our ignorance is their bliss.

HOST: Harvard professor Shoshana Zuboff is sometimes called the Karl Marx of our time. Her monumental book *The Age of Surveillance Capitalism* exposed the dubious mechanisms of our digital economy. According to Zuboff, our personal and private experiences have been hijacked by Silicon Valley and used as the raw material for extremely profitable digital products.
SHOSHANA: The term surveillance capitalism is not an arbitrary term. Why surveillance? Because it must be operations that are engineered as undetectable, indecipherable, cloaked in rhetoric that aims to misdirect, obfuscate and just downright bamboozle all of us all the time.
Tract Voice: Connecting them.
Tract Voice 2: Don't be evil.
Tract Voice: Connecting them is humanity. Don't be evil. Humanity, humanity.
Tract Voice 3: It's about empowerment of the individual.
ZUCKERBERG: The future is private.
HOST: What really happens with your Facebook photos? Why are there hidden microphones in Google Nest? And Pokemon Go exposed as child molesters? In this episode of Backlight, Shoshana Zuboff reveals how Silicon Valley deceives us so well.
QUESTIONER: How all this comes into play when I buy a pair of shoes on the internet?
SHOSHANA: Well, you know, some people will say to me, but Professor Zuboff, I like those targeted ads. They're so useful. Or I enjoy personalized services. Sometimes people will say, you know, I have nothing to hide. So I don't care what they take. Each one of these statements is a profound misconception of what's really going on.
We think that the only personal information they have about us is what we've given them and we think we can exert some control over what we give them. And therefore, we think that our calculation, our

trade-off here, is something that is somehow under our control that we understand it. What's really happening is that we provide personal information, but the information that we provide is the least important part of the information that they collect about us.

HOST: Thanks to their navigation and search engine, Google knows where we are all the time and what we think. Facebook knows our hobbies, preferences and friends because they retrieve a lot of information from the digital traces we leave behind unwittingly. Spelling errors in your search terms, which colour buttons you prefer, how fast you type, how fast you drive, residual data.

SHOSHANA: Way back at the beginning, back in the year 2000, 2001, 2002, back in those days, these data were considered just extra data. They were considered waste material. And people called them things like digital exhaust or data exhaust. Eventually, it was understood that these so-called waste materials harbored these rich predictive data.

GOOGLE EMPLOYEE: The search generation we retain, we do for quality purposes. So, for example, the Google Spell Checker, our did you mean feature that appears on Google, has been built using long periods of data around someone issuing a query and then issuing another corrected query right after that and us learning those corrections. And it actually takes more than 30 days worth of data to build the world class spell corrector that we have.

SHOSHANA: The companies like to say, we collect data so that we can improve our service. And that's true. They collect data and some of it is used to improve the service to you. But even more of it is analyzed to train what they call models, patterns of human behaviour. So once I have big training models, I can see how people with these characteristics typically behave over time. And that allows me to fit your data right into that arc and to predict what you're likely to do not only now, but soon and later. This is what I call *behavioral surplus*. These data streams filled with these rich predictive data. Why surplus? Because right from the start, these were more data than was required to improve products and services.

HOST: Once you have the behavioral surplus, the comprehensive behavioral data of hundreds of millions of people, you can start

predicting the preferences of specific groups. Think popular shoes for mail managers or the preferred restaurant of a group of people sharing the same zip code.

QUESTIONER: Maybe they do a prediction where I have dinner tonight. Or how can I imagine what they will predict about me?

SHOSHANA: Well, you know, at the simplest level, they may predict the kind of food you're in the mood for right now and then sell that prediction, auction that prediction to their business customers in the restaurant business who will then send you a very quick ad. We know you're in the mood for a delicious pasta dish tonight. We can invite you to a restaurant and here's a discount coupon.

QUESTIONER: There are some people who are saying, well, it's very improbable that those targeted ads really can achieve something because people have their own will and they will not buy some shoes just because there is an ad in front of them. **SHOSHANA:** You know, I think one of the misconceptions that it's really important for us to move away from is that surveillance capitalism is something that is only manifest in our lives when we're online or somehow it's only restricted to online targeted advertising. It's easy for us to say, oh, these things don't affect me. The fact is, this is being conducted at a layer that is not accessible to us.

HOST: We have no idea what today's algorithms can predict about us or what behavioral data they used to do it. A simple thing like buying a certain kind of shampoo can divulge essential information about us. For example, the New York Times reported a case of a supermarket chain that a new a girl was pregnant even before she did or was prepared to share the news.

The market algorithms discovered that the girl switched from fragrant shampoos to more neutral smelling products. Since the olfactory sensors of pregnant women become stronger, the market algorithm assumed this girl must be pregnant. Her father didn't know until he was repeatedly sent special offers for baby products. Thanks to the analysis of trillions of terabytes of behavioral data that we unwittingly leave around the digital domain, Big Tech sometimes knows us better than we know ourselves.

SHOSHANA: They can predict things like our personality, our emotions, our sexual orientation, our political orientation, a whole range of things that we never ever intended to disclose.
HOST: The predictive value that Big Tech can glean from residual data is huge. The family photos we post on our Facebook pages contain residual data from which vast amounts of valuable knowledge can be distilled.
SHOSHANA: Let's say I put my children's birthday party photo album on the web on the Facebook pages. What we don't understand is that the most important thing there are not the photos per se. It's the predictive signals that these companies can lift from the photos. It's not just my face, but it's allowing them to have the face so that they can analyze the hundreds of muscles in my face.
HOST: Uploading innocent snapshots on your Facebook page can have unforeseen consequences. Our faces, for example, are used to train algorithms to recognize facial features. And we have absolutely no idea what that facial recognition software is used for.
SHOSHANA: These data streams with these rich predictive signals are fed into the new factories, the computational factories, analyzed for predictions of human behavior. And these predictions are then sold. Who are they sold to? They're not sold to us. We are not the customers. They're sold to businesses, to business customers who want to maximize our value to their business, whatever it may be. They use information from our faces, which we've given billions and billions of photos to Facebook to train models for facial recognition. Those models are then sold to military operations, some of them in China. And those Chinese operations do many things, including imprisoning the Uighar, a subset of the Uighar Muslim population in China in what is rightly regarded as an open-air prison, where they actually don't have to have people behind bars because they track and follow them constantly through facial recognition.
HOST: The knowledge obtained from our residual data can be sold to anyone. Facial recognition software, for instance, might be sold to a Chinese company that supports the oppression of the Uighars in China, all that helps track down advocates of democracy in Hong Kong. That way, our precious family photos might be used by

Facebook to facilitate authoritarian regimes. And our privacy is guaranteed, because it's not our faces that are sold. It's the residual data scraped off them.

SHOSHANA: It's very difficult to have a concept of this for a very good reason. It's not because we're stupid. It's because these processes have been disguised. They operate in stealth. They have been engineered to be indecipherable, to be undetectable, to create ignorance in a vast group of all of us that they call users.

Our ignorance is their bliss. There are some things that have broken through into the public view that we do know about. So let's talk about Facebook's massive scale contagion experiments. And this is where Facebook experimented with subliminal cues planted in its Facebook pages that would actually influence offline real world behavior and emotions to see if they could make people feel happier or sadder using subliminal cues with language manipulation and word manipulation and so on.

Well, when the experimenters wrote up this work in the very prestigious scholarly journals that published the results of these experiments, they emphasized two key findings.

Number one, we now know that we can manipulate subliminal cues in the online context to change real world behavior or real world emotion. We know that we can be successful at doing this.

Number two, we can exercise this power, these methods, while bypassing user awareness.

Accented Voice: A big group of Pokemon Go players set up a meeting in Leeuwarden to stroll through the city to catch as many Pokemon as they can. In the Netherlands there are already about 1.3 million players.

SHOSHANA: Avery interesting experiment occurs in the guise of an augmented reality game called Pokemon Go.

Accented Voice: In the game you are walking around in the real world. The Pokemon are hiding in different places. You have to go to these places to collect them.

QUESTIONER: What are we not seeing when Pokemon Go is introduced in our country?

SHOSHANA: It's important to understand that Pokemon Go is an augmented reality game that was incubated, developed inside Google for many years. People being the first pioneer of surveillance capitalism, the inventor of surveillance capitalism. Pokemon Go was invented in Google, incubated there for many years, developed there, led by a man named John Hanke. And John Hanke invented an operation called Keyhole, which was invested in by the CIA and later purchased by Google and called Google Earth.

QUESTIONER: Google Earth was a CIA startup initially.

SHOSHANA: Yes, Google Earth was something called Keyhole and it was a CIA invested startup. So it's important to understand that Pokemon Go was not some happy little game that just got launched into the world by a toy company or something. When they decided to bring Pokemon Go to the public, they didn't want to bring it as a Google game. They brought it to market as Niantic Labs, which no one had ever heard of, just a cool startup with this cool game.

So now we have this Google augmented reality game and it turns out that the big game that is on top of the little game that the children are playing is a game that precisely emulates the logic of surveillance capitalism. So in surveillance capitalism, in the original version online, we predict the click-through rate and we sell the click-through rate to the advertiser who pays to get clicks on their website clicking through ultimately to the buy button. That's what they're hoping for.

Now in the real world, business customers paid Niantic Labs, the Pokemon Go company, paid Niantic Labs not for click-through but for the real world equivalent of click-through, which is called *footfall* to actually get real bodies with their real feet into real business establishments so that their feet would go fall, fall, fall, fall, tap, tap across the store or across the restaurant or across the bar in order to buy something.

QUESTIONER: So I could order by Niantic Labs a Pokemon in my ice cream bar, for instance.

SHOSHANA: All of these establishments, they're buying what are called, here's the term, *lure modules*. Modules like a gym that lure people to you, not so that they will come and be happy, but so they will come and spend money in your shop or your restaurant.

Starbucks, McDonald's, everybody was making money, everybody was making money. Niantic Labs was making money and all these businesses were making money. And the people playing the game had no idea. So they used the rewards and punishment of the game to herd you through the city to the places that were paying for your body. This was the game of Pokemon Go. This was the real game, the shadow game, getting you into a place where we have predicted that you will be. So that our predictions are worth more. If I can guarantee you're actually going to be there, my prediction that you're going to be there is worth a lot more. Economies of action are how I guarantee that. And Pokemon Go was a large-scale experiment, a global-scale experiment in economies of action, using remote control means to automate behavior, to engineer behavior, to fulfill others' commercial ends, while you are having a great time.

You are intended to be in the feeling of being served. You are intended to be saturated with convenience so that you will not notice and you will not complain. And all of this shadow operation will remain hidden because you will not ask questions because you're so busy being entertained.

So it's no longer enough to just have what you're doing online, you're browsing, you're sending messages, you're sending emails. We want to know about your walk in the park. We want to know about what you're doing in your car. We want to know about your home and what you're doing in your home.

Tract Voice 3: What if home security was different? What if it looked different?

QUESTIONER: Well, it's a beautiful system.

SHOSHANA: Some bright engineering-oriented person discovered that the Nest security system has a microphone built into it. That microphone does not figure in any schematic. When you buy the security system and it has the piece of paper that you unfold and the schematic or you go online to learn about it and there's a schematic, it does not show a microphone. It does not discuss a microphone. Now, why would you have a microphone there? Well, remember, what is our business? Our business depends upon extraction of *behavioral surplus*, scale, scope, and action. So what better device to

extract *behavioral surplus*, especially new forms, voices, conversations? What you're watching on television, what music you're listening to, who's coming in and out of your house, whether or not you're shouting at each other over the breakfast table.
All of this has tremendous predictive value. Voices are what everybody's after, just like they're after faces. So now this becomes public. There's a, hey Google, what's up with this microphone in your security system? What does Google say? Oops, so sorry. Oh, we didn't even know there was a microphone there. Oh, sorry, sorry. Somebody put that microphone there, but we never intended to use it.
This is their business to obfuscate, to misdirect, to engineer our ignorance with mechanisms and methods that are undetectable and indecipherable. And if they confront you, deny it. Deny it for as long as possible until they habituate. If there's some element that fails to get habituated, then create an adaptation.
Alright, we'll make sure all those microphones are somehow shut off so that they can't be used. And then, wait a minute, when no one is looking, redirect it. So there will be a microphone and something else. There will be a microphone in the home device or in the music player or whatever it might be. It will be back.
Tract Voice 3: What if the measure of it working? Alright guys, here we go. Daddy! Was that you never had to think about it.
SHOSHANA: There's two legal scholars that are at the University of London, and they analyze the privacy policy, how we give our consent to these devices, right? So, they analyze these documents for one Nest thermostat. What happens is the thermostat collects data. It sends those data to third parties, and those third parties send data to third parties, odd infinitum, an infinite regress, where your data is going, goodness knows where. And no company takes responsibility for what the third parties that it's sending your data to may do with your data.
And all we'll say, if you don't want us to take your data and you don't want us to send it on to third parties, that's okay. But be aware that without your data we will stop supporting the functionality of your thermostat. We will stop upgrading the software. Be aware that the

smoke detector may no longer work. Be aware that the pipes in your home may freeze.
So now the functionality of the device is held hostage to your agreeing to the privacy contract. And they say, by the way, even if you agree and we maintain the functionality, we're sending it to these other third parties, and they're going to use it the way they choose, and we take no responsibility for what they do with it.
All right. So now these two scholars do an analysis of one Nest thermostat, and what they conclude is that given these arrangements, any self-respecting consumer, anyone who's even a little bit vigilant about their consumption habits, should review a minimum of 1,000 privacy contracts in order to install just one single Nest thermostat in your home.
Google Nest commercial: You have three minutes to exit. What if it gave you time and what you really need from home security? A sense of security.

SHOSHANA: So they start extracting data at scale. First it's everything you do online, and then pretty soon they need more data, but then they also discover that we need varieties of data. It's not just volume, but it's different qualities of data.

Carlo van de Weijer (original in German): The problems in mobility are going to be the same as what we saw online with the smart phones that you are paying with your privacy without you knowing because the car knows exactly what you are doing, where you are going and any modern car will have about 15 cameras at a minimum and even if you have access to only 1% of all cars, you know what's happening all over the world.
If the data is going to be more worth than driving the car who knows, they might offer you a free car. You pay with your privacy in the same way you pay with privacy for all the free services you get from Google.
SHOSHANA: Well surveillance capitalism broke through in Silicon Valley, 2002, 2003, 2004. It changed the bar for investment. Now you had Google making money on the basis of what I call the *surveillance*

dividend. Now what venture capitalist wants to invest in a firm that's just making an app, when it can invest in a firm that's making an app plus the surveillance dividend.
So what happened right away was that the investment started flowing to the people who were making more money and that more came from the surveillance dividend. And now that is the structure that is flowing across the whole economy. Why bother to put all that effort into the engineers and the factories and the science to make a car that runs without carbon when all we need to do is sell the data from the darn vehicles. And we've got the surveillance dividend and all those investors are going to come to us and give us the kind of market capitalization that the leading surveillance capitalists have. That's our new lease on life. That's our path forward in the 20th century.
Carlo van de Weijer (original in German): The data is worth a lot that everyone is asking for it. That's why Google wants to get their products in the car, not because you can make a lot of money with a car business. You can use the car as the Trojan Horse to collect all that data.

SHOSHANA: We, even now, see it coming full circle back to the birthplace of mass production in the Ford Motor Company. Where the CEO of Ford Motor now says, you know, we want market capitalization like Facebook and Google. How do we get it? Well, instead of figuring out how to make a car that runs carbon free, what we're going to do is repurpose our automobiles as surveillance vehicles.
And we're going to stream data from the 100,000 people who are driving around in Ford cars. We're going to combine that with the data we have from Ford Credit, where he says, we already know everything about you and these data sets are going to put us on a par with the likes of the great surveillance capitalists. Who wouldn't want to invest in Ford Motor under those circumstances.
QUESTIONER: The primary economy, what we perceive as primary economy, build a nice car, grow some nice food, build a house, means zilch in this surveillance economy.

SHOSHANA: So this began with Android. Once Google acquired the ability to make the Android phone, there were a lot of people in Google who said, oh, this is fantastic. Now we have a phone like Apple, and we can sell a phone and we can make a great margin on that phone. And that margin is going to fund our profits, and this is going to make us really rich.

But the wiser heads in Google prevailed. The people who already understood surveillance capitalism prevailed and they said, just the opposite. We want the phone, and everything associated with the phone, to be as cheap as possible. In fact, if we can get the price to zero, that's even better.

We want everybody to have a phone, because the more they have the phone, and the more they spend time on the phone, the more data we get from them, the more *behavioral surplus* streams into our supply chains. So if we can give it away, we're going to give it away.

HOST: Google's free mobile operating system, Android, means Google holds the key to almost 90% of the world's smartphones. In order to obtain as much data as possible from all these cell phones, Google experimented with network balloons in those parts of the world where mobile internet is not available. Facebook, not to be outdone, flew network drones over growing markets, and offered free internet in combination with the Facebook app.

ZUCKERBERG: And connecting them represents one of the greatest opportunities available to humanity today.

AUDIENCE VOICE: Hi, Mark. Why are you showing so much interest in India? That's honestly.

ZUCKERBERG: Our mission is to give everyone in the world the power to share what's important to them and to connect every person in the world.

HOST: Aware of the potential dangers of American data robbery, India politely declined the offer, and may do without Zuckerberg's generosity. In other parts of the world, Facebook's true intentions are becoming clearer every day, but we need whistleblowers for that. Facebook is happy to take our data, but not prepared to share information on how the company works.

SHOSHANA: So this is a document written by Facebook executives in Australia, and what they told their business customers there was that we have so much data about 6.6 million Australian young adults and teenagers. As a result of that, we can predict mood shifts. We can predict when they feel stressed, fatigued, anxious, inferior, frightened, all of these kinds of very personal feelings. And we can alert you the exact moment when they are most likely to need a confidence boost.

Let's say there's a young person who's contemplating a date over the weekend, and it's now Thursday night, and their anxiety is peaking, and they need a confidence boost. If you send them an ad for a sexy black leather jacket, send it right now, offer free delivery. Tell them you'll have it at their door by the time they wake up in the morning. Give them a discount coupon.

You're going to sell that black leather jacket. Do it now. We can tell you the exact moment when they are at peak vulnerability. That is real. That's happening. And if you don't believe me, all you have to do is just pivot a few degrees to something that happened in 2018. And what is that? That came from yet another whistle blower. His name was Chris Wiley. And he told us about Cambridge Analytica.

HOST: Chris Wiley, a former employee of the British company Cambridge Analytica, sounded the alarm about the methods used by this political marketing business. Cambridge Analytica used the Facebook data of more than 18 million Americans to analyze the best ways of manipulating American voters.

SHOSHANA: One of the things that Chris Wiley said when he broke this story with the Guardian back in 2018, is he said, we knew so much about so many individuals that we could understand their inner demons. And we could figure out how to target those demons, how to target their fear, how to target their anger, how to target their paranoia.

And with those targets, we could trigger those emotions. And by triggering those emotions, we could then manipulate them into clicking on a website, joining a group, telling them what kind of things to read, telling them what kind of people to hang out with, even telling them who to vote for.

Now, that is absolutely no different than what Facebook aimed to do with these young people, innocent young people in Australia and New Zealand, to target their inner demons, the same mechanisms, the same methods, only pivoted just a few degrees from commercial outcomes to political outcomes. Cambridge Analytica was nothing but a parasite on a huge host, and that host is surveillance capitalism.

F8 Commercial: Hi, Ella. Hope you're settling in OK. You know how I always say everything you need is already within you. The truth is, there's only so much you can do by yourself. We all need people to get where we're going. Ask yourself who you're going to do it with.

ZUCKERBERG: Everyone, welcome to F8. Today, we are going to talk about building a privacy focused social platform. So that's why I believe that the future is private.

QUESTIONER: So we are all good then, Professor Zuboff.

SHOSHANA: Well, in June 2019, which happened to be just a couple of months after that grand announcement that the future is private, there's a very interesting court case that was being tried before a California judge.

And this court case was a class action suit brought by individuals who were demanding from Facebook. They wanted to have the data that Facebook had made available to Cambridge Analytica to see if they had been targeted and manipulated by Cambridge Analytica and this had come to a head in a California court.

The Facebook counsel who argued this case stood in front of the judge and said that any Facebook user gets on the platform and typically is sharing information with 100 or more people in their network.

Once you've done that, you have no expectation of privacy that would make you legitimately able to claim any kind of privacy right in a suit like this or any other kind of privacy oriented suit.

And so here we have again the public operation and the shadow operation. What's happening backstage is a lawyer standing in front of a judge saying “No Facebook user has any legitimate expectation of privacy.”

ZUCKERBERG: This is the next chapter for our services.

QUESTIONER: You have some Google products you use if I may ask you.
SHOSHANA: No.
QUESTIONER: How do you survive?
SHOSHANA: Perfectly well. If there is an occasion where I feel the absolute need to use Google, I go through various layers of encryption and location reconfiguration before I go to Google search, just on principle.
HOST: There is a way to escape the omnipresent eyes of Google and Facebook. You can use a VPN and send all your data traffic through a secure server in another country. But Big Tech won't lose any sleep over individuals resisting the surveillance capitalists.
SHOSHANA: I don't want anyone to get confused that if you forego Google search, you are somehow, you know, fighting the fight because this is a collective problem and it requires collective action.
AMISH SPEAKER: With us Amish, we are dependent on public transportation for any distance. And loads will travel. We do it in our slow way. And I think the horse and buggy slows us down and really helps the overall value that we are trying to create and preserve and not get carried away. A regular computer with your safety walls, you know, where you can't get on porn sites and things like that. Now, when our lockdowns that we have, that is totally locked down.
Tract Voice 7: Can you go on the internet with this computer?
AMISH SPEAKER: No, no, absolutely not. It will not play a movie, picture or music or anything like that. It's not a computer that was torn down. It was built from the ground up like this especially for Amish.
Tract Voice 7: Yes. Would you mind showing me your mobile phone?
AMISH SPEAKER: Okay, yes. The only thing you can do with that is call. You cannot text, do anything like that. It's just a portable phone. So this is where it stays. But as far as going home, no, I don't have it. I keep it right here. That's for the business. The technology is progressing so fast. It's hard to deal with. We have to teach what the moral impact is in being involved in this so each individual can make better choices for themselves. We use technology as long as we use it and it doesn't get to the point where it uses us and controls us. That's the bottom line of it.

QUESTIONER: It's kind of strange that these people from who you can say are living in the past, maybe they're living in the future.
SHOSHANA: It was just a minute ago that we didn't have many of these tools and we were fine. We lived rich and full lives. We had close connections and friends and family. So having said that, I want to recognize that there's a lot that the digital brings to our lives.
And we deserve to have all of that. But we deserve to have it without paying the price of surveillance capitalism. And right now, we are in that kind of classic Faustian bargain. 21st century citizens should not have to make a choice of either essentially, you know, going analog or living in a world where our self-determination, our privacy are destroyed for the sake of this market logic. That is unacceptable.
And let's also not be naive. You get the wrong people in charge of our government at any moment and they look over their shoulders at the rich control possibilities offered by these new systems. And there will come a time when even in the West, even in our democratic societies, our government will be tempted to annex these capabilities. And use them over us and against us.
Let's not be naive about that. When we decide to resist surveillance capitalism, right now, while it lives in the market dynamic, we are also preserving our democratic future and the kinds of checks and balances that we will need going forward in an information civilization if we are to preserve freedom and democracy for another generation.
HOST: The European Union already has legislation with which it regularly wraps American tech businesses over the knuckles. Google was fined several billion dollars because it had abused its monopoly position. In theory, European citizens are protected against data robbery by regulations for fair competition and by the GDPR, the General Data Protection Regulation.
QUESTIONER: And do you think that the EU data protection law is a step in a good direction or is it sufficient?
SHOSHANA: We have privacy laws And the GDPR is the furthest frontier of our privacy laws. And we have antitrust laws. The thing is that as important as these laws are, we still need more because surveillance capitalism is unprecedented.

And so we're going to need the laws and the regulatory regimes that respond directly to these new unprecedented operations. GDPR talks a lot about data ownership, data accessibility and data portability. These are very important things if the only data that we're talking about is the data in the public operation, the data that we've given to the corporations.

But as we have seen, most of the data that they use to feed into the factories, to produce the predictions, these are data that we haven't given. Or if we've given, we don't even know that we've given because it came in our exclamation points. It came in our walk in the park and picking up the cadence of our voice and the timber of our voice, all rich predictive signals.

So no matter how much data ownership we claim or accessibility or portability, most of the data is in the shadow operation and the shadow operation is never coming to us. We will never get those data. They claim them as data that they own. They took it from our lives. They took it from our private experience without our permission. They analyzed the data. They made it into products. They sold the products and they took the profit, illegitimate profit because they took it at the beginning without asking, without our knowledge, bypassing our awareness.

QUESTIONER: Do the EU have a chance against the behemoth of surveillance capitalism?

SHOSHANA: These 20 years have been the honeymoon for surveillance capitalism because they have been 20 years largely unimpeded by law, unimpeded by law. Why? Well, the most important reason is that they're doing things that have never been done before so there are no laws against it.

Just like factories employing children in a mass production factory, there hadn't been anything like that before and there were no laws against it. And it took our societies a while to sort of wake up. We stood up against the extractive companies and their violence, the companies that came to be known as the Gilded Age. The companies where we turned around and we called their leaders Robber Barons. That's not what they were called at the time. At the time they were worshiped as these wealthy gods and geniuses who knew how to

wield the might of machines and capital. If we had been trying to stop it, to curtail it, to outlaw it for every one of these 20 years and we had utterly failed, then I might, you know, put my chin in my hand and say, gosh, I'm starting to feel like things might be really bad.
But that's not the case. We haven't even tried yet to stop it. Look, surveillance capitalism is 20 years old. Democracy is several centuries old. I bet on democracy.